MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2019/2020

TSN3251 – COMPUTER SECURITY

(All sections / Groups)

24 OCTOBER 2019
9.00 a.m - 11.00 a.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of **EIGHT pages (excluding this page)** with **FIVE questions.**

2. Answer all **FIVE** questions. Each question carries **20 marks** and the distribution of the marks for each subdivision is given. Maximum allotted are **100 marks.**

3. Please write all your answers in the Answer Booklet provided.

*Answer all **FIVE** questions. Each question carries 20 marks and the distribution of the marks for each subdivision is given.* ***(5×20=100 marks)***

QUESTION 1:

a. (i) Briefly explain the following key principles of computer security, which is referred as **CIA triad.**

- Confidentiality
- Integrity
- Availability **(3 marks)**

(ii) For each of the above principles, state the **type of attack** (Interruption / Interception / Modification / Fabrication) that will affect them, with an **example** each. **(3 marks)**

b. (i) State any TWO major differences between '**Symmetric**' and '**Asymmetric**' Cryptosystems. **(4 marks)**

(ii) Draw the basic model for '**Asymmetric Cryptosystem**' to provide both authentication and secrecy. **(4 marks)**

c. State the **difference** between the following:

(i) Diffusion and Confusion

(ii) One-way Function and Trap-door one-way function

(iii) Feistel and Non-Feistel Ciphers

(3×2=6 marks)

Continued...

QUESTION 2:

a. Assume that plaintext and ciphertext characters are represented as numerical values in Z_{26} as follows:

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Answer the following questions:

(i) Assume the usage of **Multiplicative Cipher** with key **k = 19** in **modulus 26**.

- Identify the **multiplicative inverse** of the key k using extended Euclidean algorithm. **(2 marks)**

- **Decrypt** the following ciphertext using the calculated multiplicative inverse of the key.

UGNI **(4 marks)**

(ii) Use **Autokey Cipher to** encrypt the plaintext "**leader**" using the 4-character keyword "***KIND***". **(3 marks)**

b. Assume the usage of **single stage keyed block/columnar transposition cipher** and **x** as the filler character.

(i) Identify the **decryption key** if the encryption key is given as
2 4 6 1 3 5 **(2 marks)**

(ii) **Decrypt** the following ciphertext using the given cipher, and the identified decryption key in (i).
(Steps involved in Decryption: Write column by column, Permute the columns using decryption key, Read row by row)

CSOHD IEDNX NKROX ASLTR TPUAS OAEWX
(3 marks)

Continued...

c. **Euler's Totient function** (ϕ (n)) finds the number of integers that are both smaller than n and relatively prime to n.

Following rules are used for finding the value of ϕ (n).

ϕ (p) = (p-1), if p is a prime number,
ϕ (m×n) = ϕ (m)× ϕ (n) if m and n are relatively prime,
ϕ (p^e) = (p^e - p^{e-1}) if p is a prime number.

Applying the above rules, find the value of the following:

(i) **ϕ (67)** (ii) **ϕ (81)**

(2 marks)

d. Find the result of the following using the given square-and-multiply method of **fast exponentiation algorithm**.

17^{77} mod 21

```
Square_and_Multiply (a, x, n)
{
    y ← 1
    for (i ← 0 to n_b − 1)                  // n_b is the number of bits in x
    {
        if (x_i = 1)   y ← a × y mod n      // multiply only if the bit is 1

        a ← a^2 mod n                       // squaring is not needed in the last iteration
    }
    return y
}
```

(4 marks)

Continued...

QUESTION 3:

a. Answer the following questions with respect to **Data Encryption Standard (DES).**

(i) Identify the output of the **initial permutation box** in hexadecimal, when the input is given in hexadecimal as

$$\mathbf{(0000\ 0000\ 0000\ 0005)_H}$$

Initial permutation table is given below:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(2 marks)

(ii) Assume that two inputs to Substitution box (S-box) 1 are given as $\mathbf{(101100)_2}$ and $\mathbf{(010101)_2}$. Identify the corresponding outputs in binary.

Definition of S-box 1

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

(4 marks)

(iii) DES exhibits strong avalanche effect. What is meant by **avalanche effect**?

(2 marks)

(iv) State the **steps involved** in the **Meet-in-the-middle attack**, which is a known-plaintext attack on double DES.

(4 marks)

Continued...

b. Answer the following with respect to **Advanced Encryption Standard (AES-128)**.

(i) For the plaintext given below in Hexadecimal,

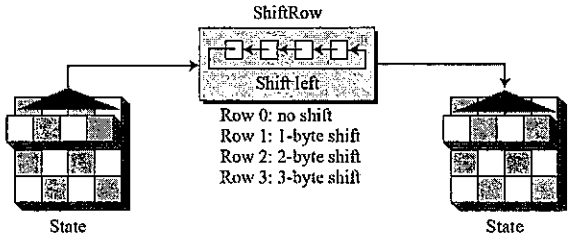
$(30\ 31\ 32\ 33\ 34\ 35\ 36\ 37\ 3F\ 3E\ 3D\ 3C\ 3B\ 3A\ 39\ 38)_H$

Identify the **original contents** of **State** as 4×4 matrix. **(2 marks)**

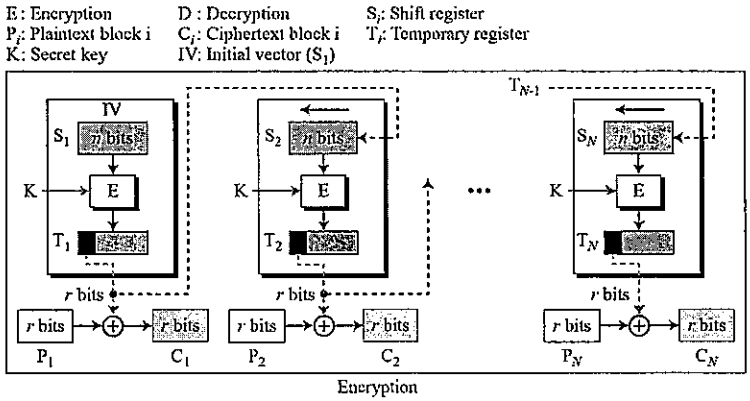
(ii) Assume that state before performing **ShiftRows transformation** on a specific round for **AES** is given below.

$$\text{State (beforeShiftRows)} = \begin{bmatrix} 60 & 61 & 62 & 63 \\ 64 & 65 & 66 & 67 \\ 68 & 69 & 6A & 6B \\ 6C & 6D & 6E & 6F \end{bmatrix}$$

Identify the **state** after performing the following Shift-Rows transformation. **(2 marks)**



c. Encryption process for **Output Feedback (OFB) mode** that can be used with modern block ciphers for enciphering text of any size is shown below.



Modify the above diagram to perform encryption, if the size of plaintext block (r) is equal to the size of the block used in block cipher (n).

(4 marks)

Continued...

QUESTION 4:

a. With reference to **Rivest-Shamir-Adleman (RSA)** cryptosystem, answer the following:

(i) Identify the **public key {e,n} and private key {d}** for the following data using RSA_Key_Generation algorithm given below.

p=7; q=11; e=13

where

p and q are two prime numbers
e is an integer with gcd (φ (n) , e) =1; 1 < e < φ (n);

(4 marks)

```
RSA_Key_Generation
{
   Select two large primes p and q such that p ≠ q.
   n ← p × q
   φ(n) ← (p − 1) × (q − 1)
   Select e such that 1 < e < φ(n) and e is coprime to φ(n)
   d ← e^−1 mod φ(n)                    // d is inverse of e modulo φ(n)
   Public_key ← (e, n)                  // To be announced publicly
   Private_key ← d                      // To be kept secret
   return Public_key and Private_key
}
```

(ii) With the help of the following algorithm, perform **encryption** using the keys derived in (i) and using the plaintext message **P = 6.**

(4 marks)

```
RSA_Encryption (P, e, n)          // P is the plaintext in Z_n and P < n
{
   C ← Fast_Exponentiation (P, e, n)   // Calculation of (P^e mod n)
   return C
}
```

Continued...

b. With reference to **program security**, answer the following:

(i) State any TWO major differences between **virus and worm.** **(2 marks)**

(ii) State the typical **phases** of operation of a **worm.** **(2 marks)**

(iii) Identify the **type of attack** in the following situation. Briefly explain your answer. **(3 marks)**

An email is received from on online air ticket reservation system, which includes original logo and inform you that you can download your tickets by logging in through the link given. You didn't book the tickets but you are the frequent traveller on the route using that airline.

c. With reference to **database security**, answer the following:

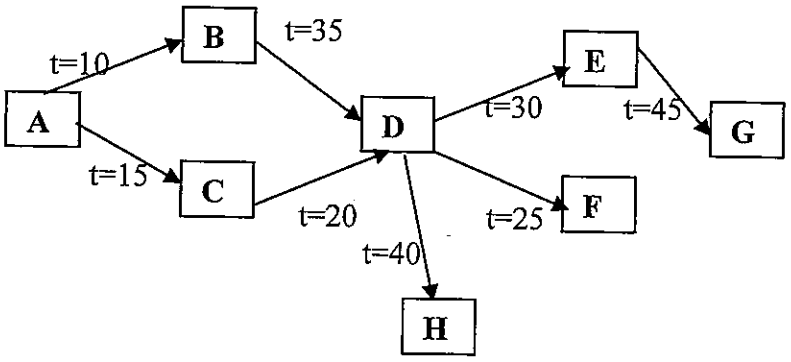
In database access control, assume that the convention followed for cascading authorization is as given below:

The grant option is used to enable an access right to cascade through a number of users. If a user has an access right with grant option, the user may pass the right to another user. When user **'S'** revokes an access right, any cascaded access right is also revoked, unless that access right would exist even if the original grant from **'S'** had never occurred. Time of grant is also considered for revoking the access right.

Answer the following question based on the above convention:

Show the resulting **diagram of access right dependencies** if the user **'C'** revokes the access right to **'D'** at **t=50** and briefly **explain** your answer.

(5 marks)



Continued...

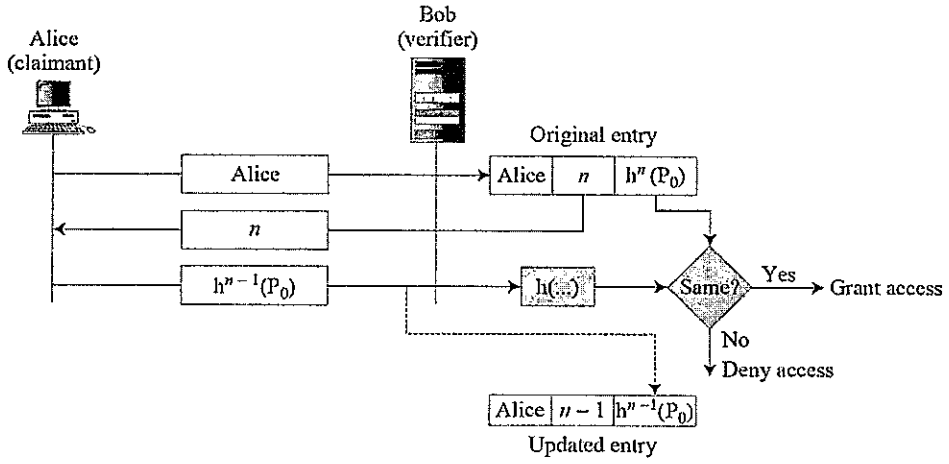
QUESTION 5:

a. With reference to **'Operating Systems Security'**, answer the following:

(i) Briefly explain how **'paging'** scheme can provide memory protection by using **valid/invalid bit,** with an example. **(4 marks)**

(ii) Give an example of an **'access matrix'** with **'switch' access right** and show how the processes can be switched from one domain to another. **(4 marks)**

(iii) Briefly explain the approach devised by Leslie Lamport for **one-time password authentication,** using the diagram given below. **(2 marks)**



b. With reference to **'Network Security'**, briefly explain the following:

(i) Phishing
(ii) Stateful and Stateless firewalls
(iii) Anomaly based Intrusion detection systems (IDS)

(2 + 2 + 2 = 6 marks)

c. Name and briefly explain any **FOUR issues** that have to be addressed by a security plan. **(4 marks)**

END OF EXAM